

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 20 juin 2000 (20.06.00)	
Demande internationale no PCT/FR99/02660	Référence du dossier du déposant ou du mandataire GEM 602
Date du dépôt international (jour/mois/année) 29 octobre 1999 (29.10.99)	Date de priorité (jour/mois/année) 29 octobre 1998 (29.10.98)
Déposant CLAVIER, Christophe etc	

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

19 mai 2000 (19.05.00)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☒ a été faite

n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé R. Forax no de téléphone: (41-22) 338.83.38
---	---

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION DE L'ENREGISTREMENT
D'UN CHANGEMENT(règle 92bis.1 et
instruction administrative 422 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

NONNENMACHER, Bernard
Gemplus
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCEDate d'expédition (jour/mois/année)
19 octobre 2000 (19.10.00)Référence du dossier du déposant ou du mandataire
GEM 602

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR99/02660Date du dépôt international (jour/mois/année)
29 octobre 1999 (29.10.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☒ le déposant ☐ l'inventeur ☐ le mandataire ☐ le représentant commun

Nom et adresse

GEMPLUS S.C.A.
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

FR

Domicile (nom de l'Etat)

FR

no de téléphone

no de télécopieur

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☐ la personne ☒ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse

GEMPLUS
Avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

FR

Domicile (nom de l'Etat)

FR

no de téléphone

no de télécopieur

no de téléimprimeur

3. Observations complémentaires, le cas échéant:

La correction du nom du déposant est également applicable à l'adresse du mandataire.

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur ☐ aux offices désignés concernés
☐ à l'administration chargée de la recherche internationale ☒ aux offices élus concernés
☒ à l'administration chargée de l'examen préliminaire international ☐ autre destinataire:Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

Fonctionnaire autorisé:

Ellen Moyse

no de téléphone (41.22) 338 83 38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

copies jointes aux documents de 26/02/00.

Expéditeur: L'ADMINISTRATION CHARGÉE DE
LA RECHERCHE INTERNATIONALE

PCT

Destinataire
GEMPLUS
Avenue du Pic de Bertagne
A l'att. de NONNENMACHER, Bernard
Parc d'activités de GEMENOS
BP 100
13881 GEMENOS Cedex
FRANCE

NOTIFICATION DE TRANSMISSION DU
RAPPORT DE RECHERCHE INTERNATIONALE
OU DE LA DECLARATION

(règle 44.1 du PCT)

REÇU le

28 JAN 2000


Date d'expédition (jour/mois/année)	26/01/2000
Référence du dossier du déposant ou du mandataire GEM 602	POUR SUITE A DONNER voir les paragraphes 1 et 4 ci-après
Demande internationale n° PCT/FR 99/02660	Date du dépôt international (jour/mois/année) 29/10/1999
Déposant GEMPLUS S.C.A. et al.	

- ☒ Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.
Dépôt de modifications et d'une déclaration selon l'article 19 :
Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale ; pour plus de précisions, voir cependant les notes figurant sur la feuille d'accompagnement.

Où? Directement auprès du Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse
n° de télécopieur: (41-22)740.14.35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.
- ☐ Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2(a), est transmise ci-joint.
- ☐ **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que
☐ la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.
☐ la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.
- Mesure(s) consécutive(s) :** Il est rappelé au déposant ce qui suit:
Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90bis.1 et 90bis.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.
Dans un délai de **19 mois** à compter de la date de priorité, le déposant doit présenter la demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit reportée à 30 mois à compter de la date de priorité (ou même au-delà dans certains offices).
Dans un délai de **20 mois** à compter de la date de priorité, le déposant doit accomplir les démarches prescrites pour l'ouverture de la phase nationale auprès de tous les offices désignés qui n'ont pas été élus dans la demande d'examen préliminaire international ou dans une élection ultérieure avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou qui ne pouvaient pas être élus parce qu'ils ne sont pas liés par le chapitre II.

Nom et adresse postale de l'administration chargée de la recherche internationale  Office Européen des Brevets, P.B. 5818 Patentaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Liliane Van Velzen-Peron
--	---

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le Guide du déposant du PCT, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou à une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains Etats.

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand?

Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment?

Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/puvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220 (suite)

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

- i) la revendication n'est pas modifiée;
- ii) la revendication est supprimée;
- iii) la revendication est nouvelle;
- iv) la revendication remplace une ou plusieurs revendications telles que déposées;
- v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 15 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."
2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
"Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."
3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."
4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1-10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendications 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demande internationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)".

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications auprès du Bureau international, déposer également une copie de ces modifications auprès de l'administration chargée de l'examen préliminaire international (voir la règle 62.2a), première phrase).

Conséquence au regard de la traduction de la demande internationale lors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle-ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du Guide du déposant du PCT.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 602	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER	
Demande internationale n° PCT/FR 99/02660	Date du dépôt international (jour/mois/année) 29/10/1999	(Date de priorité (la plus ancienne) (jour/mois/année) 29/10/1998
Déposant GEMPLUS S.C.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

a. En ce qui concerne la langue, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne les séquences de nucléotides ou d'acides aminés divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

☐ contenu dans la demande internationale, sous forme écrite.

☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

☐ remis ultérieurement à l'administration, sous forme écrite.

☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le titre,

☒ le texte est approuvé tel qu'il a été remis par le déposant.

☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,

☒ le texte est approuvé tel qu'il a été remis par le déposant

☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

☒ suggérée par le déposant.

☐ parce que le déposant n'a pas suggéré de figure.

☐ parce que cette figure caractérise mieux l'invention.

1

☐ Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 99/02660

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY"</p> <p>NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342 le document en entier</p> <p style="text-align: center;">--- -/--</p>	1,2,6,7

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- "&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

17 janvier 2000

Date d'expédition du présent rapport de recherche internationale

26/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Gautier, L

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 99/02660

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES"</p> <p>IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997 (1997-11-03), pages 689-693, XP000737626</p> <p>INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS</p> <p>abrégé</p> <p>colonne 1, ligne 13 - ligne 29</p> <p>colonne 2, ligne 6 - ligne 18</p> <p>colonne 3, ligne 1 - colonne 5, ligne 1</p> <p>---</p>	1-8
A	<p>FR 2 672 402 A (GEMPLUS CARD INT)</p> <p>7 août 1992 (1992-08-07)</p> <p>abrégé</p> <p>page 1, ligne 4 - ligne 12</p> <p>page 3, ligne 19 - ligne 23</p> <p>figure 1</p> <p>revendication 1</p> <p>-----</p>	9,10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/FR 99/02660

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2672402 A	07-08-1992	AUCUN	

PCT

REC'D 17 JAN 2001

WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL



(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire GEM 602	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/02660	Date du dépôt international (jour/mois/année) 29/10/1999	Date de priorité (jour/mois/année) 29/10/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/06		
Déposant GEMPLUS S.C.A. et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
2. Ce RAPPORT comprend 10 feuilles, y compris la présente feuille de couverture.
 - ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent 4 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:
 - I ☒ Base du rapport
 - II ☐ Priorité
 - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
 - IV ☐ Absence d'unité de l'invention
 - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
 - VI ☒ Certains documents cités
 - VII ☒ Irrégularités dans la demande internationale
 - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 19/05/2000	Date d'achèvement du présent rapport 12.01.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Grimaldo, M N° de téléphone +49 89 2399 7513 

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02660

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17.)*) :

Description, pages:

1-24 version initiale

Revendications, N°:

1-10 reçue(s) le 19/10/2000 avec la lettre du 16/10/2000

Dessins, feuilles:

1/12-12/12 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/02660

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 2-8
	Non : Revendications 1, 9, 10
Activité inventive	Oui : Revendications
	Non : Revendications 1-10
Possibilité d'application industrielle	Oui : Revendications 1-10
	Non : Revendications

2. Citations et explications
voir feuille séparée

VI. Certain documents cités

1. Certains documents publiés (règle 70.10)
et / ou

2. Divulgations non écrites (règle 70.9)

voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/02660

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Documents mentionnés

Il est fait référence aux documents suivants:

- D1: MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY", NTT REVIEW, vol. 6, no. 4, 1 juillet 1994, pages 85-90
- D2: YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES", IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997, pages 689-693, XP000737626 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

- 1a. A cause du manque des caractéristiques techniques (voir la section VIII, paragraphe 1) et du manque de clarté (voir section VIII, paragraphes 2 et 3) la formulation de la revendication 1 est trop vague.
- En conséquence de cette formulation, l'objet de la revendication 1 est connu du document D1 et la revendication 1 ne remplit pas les exigences des Articles 33(1) et (2) PCT en ce qui concerne la nouveauté.

En effet, le document D1 (pages 85-90, paragraphes 1-5) divulgue un procédé de contre-mesure contre des attaques par analyse différentielle de consommation en courant dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (modified DES) qui comprend l'utilisation de premiers moyens de traitement numérique (SBOX) [...] et la donnée de sortie et des données dérivées de cette donnée de sortie étant manipulées par des instructions dudit algorithme qui sont critiques [...].

En plus le procédé utilise d'autres moyens (differential filter and a quasi differential filter) de sorte que la donnée de sortie et les données dérivées soient imprédictibles, ces autres moyens [...] correspondant à l'application d'une opération

OU EXCLUSIF entre la donnée d'entrée des premiers moyens et une valeur aléatoire.

- 1b. Les revendications indépendantes 9 et 10, bien que formulées sous forme de revendications de dispositif (composant électrique et carte à puce) et bien qu'elles contiennent des différences mineures avec la revendication 1 (spécification d'un microprocesseur, d'une mémoire programme et d'une mémoire de travail), ne sont que des simples répétitions du contenu de la revendication de procédé 1 et ne satisfont donc pas les exigences du PCT pour les mêmes raisons (Article 33(1) et 33(3) PCT).
- 1c. Les revendications dépendantes 2-8 ne semblent pas contenir de caractéristiques supplémentaires qui, en combinaison avec l'objet de la revendication dont elles dépendent, impliqueraient une l'activité inventive (Article 33(1) et 33(3) PCT). Celles-ci sont connues, soit directement dérivables des documents cités ou soit des variantes de réalisation sans signification inventive propre.
2. Cependant, si les revendications 1, 9 et 10 sont interprétées à l'aide de la description qui spécifie les caractéristiques techniques essentielles manquantes (voir la section VIII, paragraphe 1) alors il est possible de comprendre que ces revendications concernent un procédé de contre-mesure pour protéger un algorithme DES à clé secrète d'un attaque DPA (Differential Power Analysis) (revendication 1), un composant électronique de sécurité réalisant ce procédé (revendication 9) et une carte à puce comprenant un tel composant électronique de sécurité (revendication 10).

Les algorithmes à clé secrète du type DES (Data Encryption standard) sont vulnérables aux attaques DPA consistant en une analyse différentielle de la consommation en courant, qui permettent à des tiers mal intentionnés de trouver la clé secrète.

Ces attaques sont destinées à découvrir la clé secrète en attaquant un nombre limité de bits particuliers de la clé: une sous-clé. A cette sous-clé correspondent certaines données en sortie de certaines opérations de l'algorithme de cryptographie (opérations critiques: celles qui manipulent une donnée de sortie d'une opération SBOX) qui peuvent être plus facilement prédites: les bits de ces

données sont appelés bits cibles.

Avec une attaque DPA qui analyse quand le signal DPA n'est pas nul en correspondance des instructions critiques on est capable de reconstituer la clé secrète, faisant un hypothèse sur la sous-clé.

Avec une attaque DPA sur un algorithme DES, qui utilise une clé de 64 bits, on est capable de reconstituer au moins 48 bits des 56 bits utiles de la clé secrète.

La demande présente une solution à ce problème en utilisant un procédé dans un composant électronique de sécurité qui entraîne un signal DPA nul même dans le cas où l'hypothèse de sous clé est juste car, si le signal est nul, on n'obtient aucune information sur le bits cibles et donc sur la clé secrète. De cette façon rien ne permet de distinguer le cas de l'hypothèse de sous-clé juste des cas d'hypothèse de sous-clés fausses. En plus, la présente invention entraîne un signal DPA toujours nul quel que soit le nombre de bits cible pris, quelle que soit la combinaison de paquets effectuée pour faire la comparaison des consommations moyens.

Le signal DPA nul est obtenu par:

- a) avant une instruction critique, une opération de OU EXCLUSIF entre la donnée d'entrée de l'opération critique et une valeur aléatoire (u) ou une valeur dérivée de cette valeur aléatoire ($e(p(u))$);

et/ou

- b) après l'instruction critique, une opération de OU EXCLUSIF entre la donnée de sortie de l'opération critique et une valeur aléatoire (u) ou une valeur dérivée de cette valeur aléatoire ($e(p(u))$);

Le document D1, considéré comme représentant l'état de la technique le plus pertinent, divulgue également un algorithme à clé secrète du type DES modifié pour supporter une attaque différentielle (page 85, colonne de droite, lignes 1-11). Cependant la modification de l'algorithme DES apportée dans la demande est différente de la modification divulguée dans le document D1.

Dans le document D1 les tables de constantes élémentaires S1 à S8 d'une opérations SBOX sont changés dynamiquement entre elles par substitutions/permutations par l'introduction d'un paramètre adjoint: le paramètre est la clé secrète.

Dans la demande presente, une opération de OU EXCLUSIF entre la donnée et

une valeur aléatoire ou une valeur dérivée de cette valeur aléatoire est appliquée avant et/ou après une instruction critique, c'est-à-dire à la sortie d'une opération SBOX.

La solution n'est donc ni connue ni dérivable du document le plus proche (D1), et donc, des revendications indépendantes 1, 9 et 10 contenant les caractéristiques techniques manquantes pourraient être considérées comme nouvelles et impliquant une activité inventive.

VI. Certains documents publiés (règle 70.10)

Demande n° Brevet n°	Date de publication (jour/mois/année)	Date de dépôt (jour/mois/année)	Date de priorité (valablement revendiquée) (jour/mois/année)
WO 00 24155	27/04/2000	13/09/1999	16/10/1998
WO 00 24156	27/04/2000	15/09/1999	16/10/1998

VII. Irrégularités dans la demande internationale

- 1a. En vue de remplir les conditions énoncées à la Règle 5.1(a)(ii) PCT, le Demandeur aurait dû citer **dans la description** les documents D1 et D2, qui semblent être les plus pertinents, et d'indiquer l'état correspondant de la technique.
- 1b. Le Demandeur aurait dû également citer dans la description les documents de la section VI et mentionner leur date de publication.
2. En vue de faciliter la compréhension des revendications, celles-ci auraient dû contenir des signes de référence entre parenthèses, que ce soit dans le préambule ou dans la partie caractérisante (Règle 6.2(b) PCT).

VIII. Observations relatives à la demande internationale

1. Il ressort clairement de la description (page 14, ligne 5 - page 15, ligne 17 et figures 3 et 8) que les caractéristiques suivantes sont essentielle à la définition de l'invention pour les revendications 1 et 9:

a) la définition des "premiers moyens" en opération SBOX;

OU

b) la définition détaillée des "données dérivées" ET des "instructions critiques".

Les raisons en sont les suivantes:

La définition des premier moyens ou des données dérivées et des instructions critiques est nécessaire pour déterminer les données particulières sur lesquelles la nouvelle opération de OU EXCLUSIF est appliquée.

Si le Demandeur ne définit pas au moins une des ces caractéristiques (a ou b), il serait possible d'interpréter, par exemple, la revendication 1 d'une façon générale où certaines données (d'entrée et de sortie des premiers moyens) subissent simplement et seulement une opération de OU EXCLUSIF. Cette interprétation n'est pas inventive eu égard, par exemple, au document D1 (voir aussi section V, paragraphe 1a et 1b).

En introduisant ces caractéristiques l'homme du métier pourrait exactement positionner l'opération de OU EXCLUSIF dans le procédé de contre-mesure revendiquée en connaissant:

a) les "premiers" moyens, à la sortie desquels l'opération critique est positionnée et, donc, l'opération de OU EXCLUSIF est appliquée;

OU

b) les données dérivées qui manipulées par les instructions critiques permettent à l'homme du métier de connaître la position de la donnée d'entrée sur laquelle s'applique l'opération de OU EXCLUSIF.

Les revendications indépendantes 1 et 9 ne contenant pas ces caractéristiques, ne remplissent pas la condition visée à l'Article 6 PCT en combinaison avec la règle 6.3 b) PCT, qui prévoient qu'une revendication indépendante doit contenir toutes les caractéristiques techniques essentielles à la définition de l'invention.

2. L'objet de la revendication 1 n'est pas clairement défini (article 6 PCT). Les expressions suivantes sont vagues et équivoques, et laissent un doute quant à la signification des caractéristiques techniques auxquelles elles se réfèrent: "utilise d'autre moyen (TC1) de façon alternative avec lesdits premiers moyens" et "ces autres moyens définis à partir desdits premiers moyens":
il n'est pas possible de comprendre si les "autres moyens" remplacent les "premiers moyens" ou si les "autres moyens" sont appliqués en série avant des "premiers moyens" ou si les "autres moyens" sont appliqués en série après des "premiers moyens".
3. L'objet des revendications 1 et 9 n'est pas clairement défini (Article 6 PCT). Les expressions suivantes sont vagues et équivoques, et laissent un doute quant à la signification des caractéristiques techniques auxquelles elles se réfèrent:
- i) "pour faire correspondre à la donnée d'entrée, une donnée de sortie...":
 - il n'est pas possible de comprendre si la donnée d'entrée est la donnée d'entrée des autres moyens ou des premiers moyens;
 - il n'est pas possible de comprendre à quelle donnée correspond cette donnée d'entrée: à la donnée de sortie des premiers moyens? à la donnée de série des autres moyens? à une donnée de sortie d'une opération de OU EXCLUSIF?
 - ii) "une opération de OU EXCLUSIF entre donnée d'entrée et (la donnée) de sortie desdits premiers moyens...":
il n'est pas possible de comprendre si l'opération, qui correspond aux "autres moyens", est appliquée entre la donnée d'entrée et la donnée de sortie des premiers moyens ou entre la donnée d'entrée des premiers moyens et une valeur aléatoire ou entre la donnée de sortie des premiers moyens et une valeur aléatoire.

NOUVELLES REVENDICATIONS

1. Procédé de contre-mesure contre des attaques par analyse différentielle de consommation en courant dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K), la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens de traitement numérique (TC_0) pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), la donnée de sortie et/ou des données dérivées de cette donnée de sortie étant manipulées par des instructions dudit algorithme, qui sont critiques au sens des dites attaques, caractérisé en ce que le procédé de contre-mesure utilise d'autres moyens (TC_1) de façon alternative avec lesdits premiers moyens, en sorte que la donnée de sortie et les données dérivées soient imprédictibles, ces autres moyens étant définis à partir des dits premier moyens, pour faire correspondre à la donnée d'entrée, une donnée de sortie correspondant à l'application d'une opération OU EXCLUSIF entre la donnée d'entrée et/ou de sortie desdits premiers moyens et une valeur aléatoire (u) ou une valeur dérivée de cette valeur aléatoire ($e(p(u))$).

2. Procédé de contre-mesure selon la revendication 1, la mise en oeuvre de l'algorithme comprenant seize tours de calcul (T_1, \dots, T_{16}), chaque tour utilisant des premiers moyens (TC_0) pour fournir une donnée de sortie à partir d'une donnée d'entrée, la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques dans les trois premiers (T_1, T_2, T_3) et les trois derniers tours (T_{14}, T_{15}, T_{16}), caractérisé en ce que l'on forme un groupe (G_1) comprenant les trois premiers tours au moins et un

autre groupe (G4) comprenant les trois derniers tours au moins, et en ce que l'on associe au premier groupe (G1) et au dernier groupe (G4) une séquence d'exécution (SEQA) utilisant les autres moyens (TC₁, TC₂) dans
5 certains tours au moins.

3. Procédé de contre-mesure selon la revendication 2, caractérisé en ce que l'on forme quatre groupes (G1,...G4) de quatre tours successifs chacun (T1,...T4)
10 et , en ce que l'on applique au moins au premier groupe (G1) et au dernier groupe (G4) la dite séquence d'exécution (SEQA).

4. Procédé de contre-mesure selon la revendication
15 3, caractérisé en ce que la dite séquence (SEQA) est exécutée dans chacun des groupes (G1,...G4).

5. Procédé de contre-mesure selon la revendication 2, caractérisé en ce que la dite séquence d'exécution (SEQA) est appliquée à un premier groupe (G1) formé des
20 trois premiers tours (T1, T2, T3) et à un dernier groupe formé des trois derniers tours (T14, T15, T16).

6. Procédé de contre-mesure selon l'une quelconque
25 des revendications précédentes, caractérisé en ce que chaque exécution de l'algorithme comprend le tirage d'une valeur aléatoire (u), et le calcul des autres moyens.

30 7. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens sont des tables de constantes.

8. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens sont utilisés en combinaison avec une opération OU exclusif supplémentaire (CP) avec la
5 valeur aléatoire ou une valeur dérivée ($p(u)$, $e(p(u))$).

9. Composant électronique de sécurité comprenant un microprocesseur, une mémoire programme et une mémoire de travail permettant la mise en oeuvre d'un algorithme
10 cryptographique à clé secrète (K), des premiers moyens (TC_0) de traitement numérique fixés en mémoire programme étant prévus pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), ladite donnée de sortie et/ou des données dérivées de cette
15 donnée de sortie étant manipulées par des instructions critiques dudit algorithme au sens d'attaques par analyse différentielle de consommation en courant, caractérisé en ce qu'il comprend des moyens de mise en oeuvre d'un procédé de contre-mesure contre lesdites
20 attaques selon l'une quelconque des revendications 1 à 8 précédentes, comprenant des moyens (4) de génération d'une valeur aléatoire (u), et d'autres moyens (TC_1 , TC_2) de traitement numérique mémorisés en mémoire de travail (3), ces moyens étant calculés à chaque
25 nouvelle exécution de l'algorithme à partir des données d'entrée et/ou de sortie des dits premiers moyens et une valeur aléatoire (u), pour faire correspondre à la donnée d'entrée, une donnée de sortie correspondant à l'application d'une opération OU EXCLUSIF entre la
30 donnée d'entrée et/ou de sortie desdits premiers moyens et une valeur aléatoire (u) ou une valeur dérivée de cette valeur aléatoire ($e(p(u))$).

10. Carte à puce comprenant un composant électronique de sécurité selon la revendication 9.